

CLAIMS

1. A method for use with a postage meter system under the jurisdiction of a postal authority, the postage meter system comprising a host and a server, the host comprising a postal security device and postal indicia printing means, the server comprising cryptographic device disposed for
5 cryptographically secure communication with the postal security device, the method comprising the steps of:

entering information into the host indicative of a batch of mail pieces to be franked;

franking the mail pieces whilst storing information about the franking of the batch of mail pieces to a memory within the host;

10 within the postal security device, performing a cryptographic authenticating procedure upon the information about the franking of the batch and the information indicative of the batch, said information defining statistical information;

communicating the statistical information from the postal security device to the cryptographic device;

15 authenticating the statistical information at the cryptographic device; and

passing the statistical information to a postal authority.

2. The method of claim 1 wherein the step of performing the cryptographic authenticating procedure comprises calculating a message authentication code, and the step of authenticating the statistical information comprises checking for correctness of the message authentication code.

20 3. The method of claim 1 wherein the step of performing the cryptographic authenticating

procedure comprises digitally signing the statistical information, and the step of authenticating the statistical information comprises checking for correctness of the digital signature.

4. The method of claim 1 wherein the communicating step further comprises establishing a cryptographically secure session and communicating the information in a cryptographically secure fashion.

5. The method of claim 1 wherein the communicating step is performed in the absence of the establishment of a cryptographically secure session.

6. The method of claim 1 further comprising the step of passing a confirmation from the cryptographic device to the postal security device indicative of receipt by the cryptographic device from the postal security device, and the further step of deleting the statistical information from the postal security device upon receipt of the confirmation.

7. The method of claim 1 further comprising the step, performed by the postal authority, of granting a discount based on the statistical information.

8. The method of claim 1 further comprising the step, performed by the postal authority, of granting a credit for future franking based on the statistical information.

9. The method of claim 1 wherein the memory within the host is within the postal security device.

10. The method of claim 1 wherein the memory within the host is not within the postal security device.

11. The method of claim 1 where the step of communicating the statistical information from the postal security device to the cryptographic device further comprises the steps of:

cryptographically signing the statistical information within the postal security device, yielding a signature;

communicating the information and signature to memory within the host and not within the postal security device;

5 storing the information and signature within the memory within the host and not within the postal security device, and

communicating the information and signature from memory within the host and not within the postal security device, to the cryptographic device.

10 12. The method of claim 11 wherein the storing of the information and signature within the memory within the host and not within the postal security device is for at least one day.

15 13. A method for use with a postage meter system under the jurisdiction of a postal authority, the postage meter system comprising a host and a server, the host comprising a postal security device and postal indicia printing means, the server comprising cryptographic device disposed for cryptographically secure communication with the postal security device, the host operated by a service provider providing service to a plurality of users, the method comprising the steps of:

entering information into the host indicative of a batch of mail pieces to be franked and indicative of an identity of a user associated with the batch;

franking the mail pieces whilst storing information about the franking of the batch of mail pieces to a memory within the host;

20 within the postal security device, performing a cryptographic authenticating procedure upon the information about the franking of the batch and the information indicative of the batch, said

information defining statistical information;

communicating the statistical information from the postal security device to the cryptographic device;

authenticating the statistical information at the cryptographic device; and

5 passing the statistical information to a postal authority.

14. The method of claim 13 wherein the step of performing the cryptographic authenticating procedure comprises calculating a message authentication code, and the step of authenticating the statistical information comprises checking for correctness of the message authentication code.

10 15. The method of claim 13 wherein the step of performing the cryptographic authenticating procedure comprises digitally signing the statistical information, and the step of authenticating the statistical information comprises checking for correctness of the digital signature.

16. The method of claim 13 wherein the communicating step further comprises establishing a cryptographically secure session and communicating the information in a cryptographically secure fashion.

15 17. The method of claim 13 wherein the communicating step is performed in the absence of the establishment of a cryptographically secure session.

18. The method of claim 13 further comprising the step of passing a confirmation from the cryptographic device to the postal security device indicative of receipt by the cryptographic device from the postal security device, and the further step of deleting the statistical information from the postal security device upon receipt of the confirmation.

19. The method of claim 13 further comprising the step, performed by the postal authority, of granting a discount to the user associated with the batch based on the statistical information.

20. The method of claim 13 further comprising the step, performed by the postal authority, of granting a credit for future franking to the user associated with the batch based on the statistical information.

21. The method of claim 13 wherein the memory within the host is within the postal security device.

22. The method of claim 13 wherein the memory within the host is not within the postal security device.

23. The method of claim 13 where the step of communicating the statistical information from the postal security device to the cryptographic device further comprises the steps of:

cryptographically signing the statistical information within the postal security device, yielding a signature;

communicating the information and signature to memory within the host and not within the postal security device;

storing the information and signature within the memory within the host and not within the postal security device, and

communicating the information and signature from memory within the host and not within the postal security device, to the cryptographic device.

24. The method of claim 23 wherein the storing of the information and signature within the

memory within the host and not within the postal security device is for at least one day.